

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 3 2 1 5 8 1
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 2 1 5 8 1]

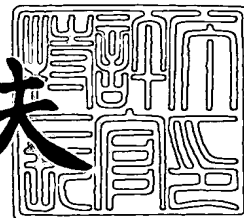
出 願 人 シャープ株式会社
Applicant(s):



2 0 0 3 年 1 0 月 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 02J02715

【提出日】 平成14年11月 5日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 9/00
G06T 1/00

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号シャープ株式会社
会社内

【氏名】 貫野 浩司

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【代理人】

【識別番号】 100084135

【弁理士】

【氏名又は名称】 本庄 武男

【手数料の表示】

【予納台帳番号】 001993

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理システム、スキャナ及び端末装置

【特許請求の範囲】

【請求項 1】 原稿画像を読み取るスキャナと、上記スキャナに対して該スキャナへの操作指令を送信するべく、上記スキャナと通信可能に接続されてなる端末装置とを具備してなる画像処理システムにおいて、

上記スキャナは、少なくとも操作者の指紋情報を読み取る第 1 の指紋情報読取手段と、上記第 1 の指紋情報読取手段により読み取られた指紋情報を一時的に記憶する第 1 の指紋情報記憶手段とを具備し、

上記端末装置は、少なくとも操作者の指紋情報を読み取る第 2 の指紋情報読取手段と、上記第 2 の指紋情報読取手段により読み取られた指紋情報を一時的に記憶する第 2 の指紋情報記憶手段とを具備し、

上記スキャナ或いは上記端末装置が、上記スキャナと上記端末装置が通信して、上記スキャナ側の第 1 の指紋情報記憶手段により記憶された指紋情報と、上記端末装置側の第 2 の指紋情報読取手段により記憶された指紋情報とを照合する指紋情報照合手段及び／若しくは、上記指紋情報照合手段による照合結果に基づいて、上記端末装置で入力された操作指令による上記スキャナの操作を許可する操作許可手段を具備することを特徴とする画像処理システム。

【請求項 2】 上記操作許可手段が、上記照合が合致する場合に上記端末装置で入力された操作指令による上記スキャナの操作を許可するものである、請求項 1 に記載の画像処理システム。

【請求項 3】 当該画像処理システムが、少なくとも上記スキャナへ操作指令を出す前に原稿画像を読み取る原稿画像読取手段と、該原稿画像読取手段により読み取られた原稿画像情報と、上記第 1 の指紋情報読取手段により読み取られた指紋情報とを関連付けた関連情報を作成する関連情報作成手段と、上記関連情報作成手段により作成された関連情報を記憶する関連情報記憶手段とを更に具備するものである、請求項 1 又は 2 に記載の画像処理システム。

【請求項 4】 当該画像処理システムが、上記関連情報記憶手段を備えるサーバを更に具備するものである、請求項 1 ～ 3 のいずれかに記載の画像処理システ

ム。

【請求項 5】 当該画像処理システムが、

上記原稿画像読取手段により読み取られた原稿画像情報と、過去の上記関連情報に含まれる画像情報とを照合する関連画像情報照合手段と、

上記第 1 の指紋情報読記憶手段で記憶された指紋情報と、過去の上記関連情報に含まれる指紋情報とを照合する関連指紋情報照合手段と、

上記関連画像照合手段による照合が合致し、且つ、上記関連指紋情報照合手段による照合が合致しない場合は、上記スキャナの操作を禁止する操作禁止手段とを更に具備してなる、請求項 1 ～ 4 のいずれかに記載の画像処理システム。

【請求項 6】 当該画像処理システムが、上記関連情報を消去する関連情報消去手段を更に具備してなる、請求項 1 ～ 5 のいずれかに記載の画像処理システム。

【請求項 7】 上記関連情報消去手段が、操作終了前に原稿が取り出された場合には、該原稿に関して作成された関連情報を消去しないものである、請求項 1 ～ 6 のいずれかに記載の画像処理システム。

【請求項 8】 上記関連情報消去手段が、所定の時限経過後に上記関連情報を消去するものである、請求項 1 ～ 7 のいずれかに記載の画像処理システム。

【請求項 9】 原稿画像を読み取るスキャナと、上記スキャナに対して該スキャナへの操作指令を送信するべく、上記スキャナと通信可能に接続されてなる端末装置とを具備してなる画像処理システムに用いられるスキャナにおいて、

少なくとも操作者の指紋情報を読み取る第 1 の指紋情報読取手段と、

上記第 1 の指紋情報読取手段により読み取られた指紋情報を一時的に記憶する第 1 の指紋情報記憶手段と、

上記スキャナと上記端末装置が通信して、上記スキャナ側で取得された指紋情報と、上記端末装置側で取得された指紋情報とを照合する指紋情報照合手段と、

上記指紋情報照合手段による照合結果に基づいて、上記端末装置で入力された操作指令による上記スキャナの操作を許可する操作許可手段とを、具備することを特徴とするスキャナ。

【請求項 10】 原稿画像を読み取るスキャナと、上記スキャナに対して該ス

キャナへの操作指令を送信するべく、上記スキャナと通信可能に接続されてなる端末装置とを具備してなる画像処理システムに用いられる端末装置において、

少なくとも操作者の指紋情報を読み取る第 2 の指紋情報記憶手段と、

上記第 2 の指紋情報記憶手段により読み取られた指紋情報を一時的に記憶する第 2 の指紋情報記憶手段と、

上記スキャナと上記端末装置が通信して、上記スキャナ側で取得された指紋情報と、上記端末装置側で取得された指紋情報とを照合する指紋情報照合手段と、上記指紋情報照合手段による照合結果に基づいて、上記端末装置で入力された操作指令による上記スキャナの操作を許可する操作許可手段とを、具備することを特徴とする端末装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、端末装置からの操作指令に基づいて原稿画像を読み取るにあたり、操作者の指紋情報を利用して原稿画像の読取許可を行う画像処理システム、スキャナ及び端末装置に関するものである。

【0 0 0 2】

【従来の技術】

一般的に上記画像処理システムに用いられるスキャナには、スキャナ側から送信先の端末装置を指定して原稿読取画像を送信するプッシュ型と、端末装置側からスキャナに操作指令を送信し、スキャナを操作することにより、原稿読取画像を端末装置に転送させるプル型がある。

また、ネットワークに接続する際には、セキュリティ保護のためパスワードを入力する方法が一般的に採用されている。

従来、例えば特許文献 1 に示されるように、プッシュ型スキャナにおいて、原稿画像の読み取りを指示する操作部に、スキャナ操作者の指紋情報を読み取るための指紋読取部を設け、上記操作部が押下されるとともに上記指紋読取部によって操作者の指紋情報を読み取ることにより、予め登録された指紋情報と操作者の指紋情報とが一致する場合に、操作者の端末装置に原稿読取画像を送信するよう

制御された画像処理装置がある。これにより、操作者はスキャナ側で送信先の端末装置の指定及び、セキュリティ保護のためのパスワード入力作業をワンタッチで行うことが可能になる。

そしてまた、操作者の指紋情報を利用したプル型の通信形体を持つものに、例えば特許文献 2 に示されるように、読み取られた指紋情報が予め登録された指紋情報と一致している場合にのみ、操作者がコンピュータを使用する、或いは、ネットワークに接続すること等を認める認証方法が提案されている。

【 0 0 0 3 】

【特許文献 1】

特開 2001-45192 号公報

【特許文献 2】

特開平 11-95921 号公報

【 0 0 0 4 】

【発明が解決しようとする課題】

しかしながら、取得した画像の読取条件の確認は、プッシュ型、プル型のいずれの場合であっても端末装置側で行わなければならないところ、特許文献 1 に記載されている技術では、プッシュ型であるために、取得した画像の読取条件（解像度、画像の大きさ等）が気に入らないものである場合には、そのつど何度も操作者がスキャナの設置場所まで行って読取操作をしなければならないという問題があるのに加えて、予め操作者の指紋情報を操作者の端末装置に関連付けてサーバ等の記憶部に保存登録しておく必要があった。そのため、未登録者は指紋情報を新たに保存登録しなければスキャナを使用することができないという問題があった。

更に、操作者の指紋情報を保存登録することは、指紋情報がネットワークに接続されたサーバ等の記憶部に常に保存された状態を意味し、現在のネットワーク技術ではセキュリティ上必ずしも安全とはいえず、重要な個人情報である指紋情報が外部に流出する危険性と、それに対する指紋登録者の不安が常に付きまとうという問題があった。

一方、一般的に、プル型スキャナでは、読み取った原稿画像を、操作指令をす

る端末装置側ですぐさま確認することができ、例えば読み取った画像が気に入らなければ、納得のいく画像を得るまで容易に再読取をすることができるという利点を有する。しかしその反面、原稿をスキャナにセットしたままで、スキャナ設置場所から離れた端末装置側で操作指令を行う必要があるため、原稿そのものを盗用されるだけでなく、ネットワークに接続された他の端末操作者により容易に原稿画像を読み取られる恐れがあった。

従って、本発明は上記事情に鑑みてなされたものであり、その第1の目的とするところは、スキャナ側で最初に読取操作をした操作者のみだけが、端末装置からそのスキャナにセットされた原稿を読み取りることができるようにして、画像情報の盗難に対するセキュリティを向上させることである。

また、第2の目的とするところは、上記スキャナにセットされた原稿が、他のスキャナで読み取られることを未然に防止することで、セキュリティの向上を図ることである。

更に、第3の目的とするところは、重要な個人情報である指紋情報をできるだけサーバ等の記憶装置に長期保存せず、従来と比べてより高いセキュリティ性と操作性を有する画像処理システムを提供することにある。

【0005】

【課題を解決するための手段】

上記目的を達成するために本発明は、原稿画像を読み取るスキャナと、上記スキャナに対して該スキャナへの操作指令を送信するべく、上記スキャナと通信可能に接続されてなる端末装置とを具備してなる画像処理システムにおいて、上記スキャナは、少なくとも操作者の指紋情報を読み取る第1の指紋情報読取手段と、上記第1の指紋情報読取手段により読み取られた指紋情報を一時的に記憶する第1の指紋情報記憶手段とを具備し、上記端末装置は、少なくとも操作者の指紋情報を読み取る第2の指紋情報読取手段と、上記第2の指紋情報読取手段により読み取られた指紋情報を一時的に記憶する第2の指紋情報記憶手段とを具備し、上記スキャナ或いは上記端末装置が、上記スキャナと上記端末装置が通信して、上記スキャナ側の第1の指紋情報記憶手段により記憶された指紋情報と、上記端末装置側の第2の指紋情報読取手段により記憶された指紋情報とを照合する指紋

情報照合手段及び／若しくは、上記指紋情報照合手段による照合結果に基づいて、上記端末装置で入力された操作指令による上記スキャナの操作を許可する操作許可手段を具備することを特徴とする画像処理システムとして構成されている。

このように構成されることによって、指紋情報を利用して操作者の認証をすることができるため、セキュリティ性の高い画像処理システムを提供することができる。また、予め登録された操作者に限られず、何人も上記スキャナを使用することが可能となるので、操作性の向上が図られる。そのためには、上記操作許可手段は、上記照合が合致する場合に許可するものであることが好ましい。

【0006】

ここで、当該画像処理システムが、少なくとも上記スキャナへ操作指令を出す前に原稿画像を読み取る原稿画像読取手段と、該原稿画像読取手段により読み取られた原稿画像情報と、上記第1の指紋情報読取手段により読み取られた指紋情報とを関連付けた関連情報を作成する関連情報作成手段と、上記関連情報作成手段により作成された関連情報を記憶する関連情報記憶手段とを更に具備するものであってもよい。

指紋情報と原稿画像とが関連付けられているので、たとえ原稿自体が盗まれたとしても、関連付けられた指紋情報があることを理由に、盗難原稿の画像情報の読み取りを禁止することが可能となり、原稿画像の盗用を防止する効果を奏する。

【0007】

従って、この場合は、当該画像処理システムは、上記原稿画像読取手段により読み取られた原稿画像情報と、過去の上記関連情報に含まれる画像情報とを照合する関連画像情報照合手段と、上記第1の指紋情報読記憶手段で記憶された指紋情報と、過去の上記関連情報に含まれる指紋情報とを照合する関連指紋情報照合手段と、上記関連画像照合手段による照合が合致し、且つ、上記関連指紋情報照合手段による照合が合致しない場合は、上記スキャナの操作を禁止する操作禁止手段とを更に具備するものであるほうがよい。

このように構成されることで、関連付けられた指紋情報の持ち主だけが、関連情報と一致する原稿を読み取ることができ、第三者が該画像情報を読み取る行為

を有効に禁止することができる。

【 0 0 0 8 】

更に、当該画像処理システムが、上記関連情報記憶手段を備えるサーバを更に具備するものが考えられる。

例えば上記関連情報を、上記スキャナや上記端末装置と通信可能なサーバに記憶させることによって、他のスキャナにおいて、第三者が上記盗難原稿の画像情報を読み取る行為をも禁止することができる。

【 0 0 0 9 】

また、当該画像処理システムが、上記関連情報を消去する関連情報消去手段を更に具備することで、例えば、操作終了後に、一時的に記憶された指紋情報等を消去することが可能となり、操作者の重要な個人情報である指紋情報が保存されないので、該指紋情報が外部に流出する危険性がなくなり、同時に指紋保有者の不安も解消されることになる。

【 0 0 1 0 】

上記関連情報消去手段が、操作終了前に原稿が取り出された場合には、該原稿に関して作成された関連情報を消去しないものであることが好ましい。

これにより例えば原稿が盗難された場合には、該原稿の関連情報が残存し、かかる関連情報は指紋情報と関連付けられているため、該指紋情報と一致しない第三者によって該原稿の画像情報を読み取られないようにすることが可能となる。

【 0 0 1 1 】

また、上記関連情報消去手段が、所定の時限経過後に上記関連情報を消去するものであってもよい。スキャナが長時間独占使用されることも考えられるため、所定の時間が経過した場合には、そのような独占使用を排除すべくスキャナ操作を強制中断させることができ、その結果、円滑な画像処理システムの運用を図ることができる。

【 0 0 1 2 】

また、前記課題は、下記スキャナによっても解決され得る。

即ち、前記課題の解決のために、原稿画像を読み取るスキャナと、上記スキャナに対して該スキャナへの操作指令を送信すべく、上記スキャナと通信可能に

接続されてなる端末装置とを具備してなる画像処理システムに用いられるスキャナにおいて、少なくとも操作者の指紋情報を読み取る第1の指紋情報読取手段と、上記第1の指紋情報読取手段により読み取られた指紋情報を一時的に記憶する第1の指紋情報記憶手段と、上記スキャナと上記端末装置が通信して、上記スキャナ側で取得された指紋情報と、上記端末装置側で取得された指紋情報とを照合する指紋情報照合手段と、上記指紋情報照合手段による照合結果に基づいて、上記端末装置で入力された操作指令による上記スキャナの操作を許可する操作許可手段とを具備することを特徴とするスキャナが提供される。

【0013】

更にまた、前記課題は、下記端末装置によっても解決され得る。

つまり、前記課題解決のために、原稿画像を読み取るスキャナと、上記スキャナに対して該スキャナへの操作指令を送信するべく、上記スキャナと通信可能に接続されてなる端末装置とを具備してなる画像処理システムに用いられる端末装置において、少なくとも操作者の指紋情報を読み取る第2の指紋情報記憶手段と、上記第2の指紋情報記憶手段により読み取られた指紋情報を一時的に記憶する第2の指紋情報記憶手段と、上記スキャナと上記端末装置が通信して、上記スキャナ側で取得された指紋情報と、上記端末装置側で取得された指紋情報とを照合する指紋情報照合手段と、上記指紋情報照合手段による照合結果に基づいて、上記端末装置で入力された操作指令による上記スキャナの操作を許可する操作許可手段とを具備することを特徴とする端末装置が提供される。

【0014】

【発明の実施の形態】

以下添付図面を参照しながら、本発明の実施の形態及び実施例について説明し、本発明の理解に供する。尚、以下の実施の形態及び実施例は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

ここに、図1は本発明の実施の形態に係る画像処理システムの全体構成を表すブロック図、図2は本発明の実施の形態に係る画像処理システムにより実行される原稿画像の読み取りを行う処理手順を表すフローチャート。図3、4は本発明の実施例に係る画像処理システムにより実行される原稿画像の読み取りを行う処

理手順を表すフローチャート、図 5 は本発明の実施の形態に係る画像処理システムに用いられるスキャナ X の操作パネルの一例を表した図である。

【 0 0 1 5 】

まず、図 1 を用いて、本発明の実施の一形態に係る画像処理システムの構成について説明する。

本画像処理システムは、スキャナ X と、サーバ 2 0 と、ホストコンピュータ（以下、「ホスト P C」と称す）3 0、4 0 に接続され、それぞれが通信可能な状態で構成されている。

サーバ 2 0 は、関連情報等を記憶する記憶部 2 1 を具備し、ネットワークに接続されている各種端末装置を統括管理する役割を果たすものである。

ホスト P C 3 0、4 0 は端末装置の一例であり、操作者の指紋を読み取るための指紋読取部 3 1（第 2 の指紋情報読取手段の一例）と、上記指紋読取部 3 1 で読み取られた指紋情報を一時的に格納する指紋情報記憶部 3 3（第 2 の指紋情報記憶手段の一例）と、スキャナ X に操作指令を送信するためのスキャナドライバ 3 2 と、上記指紋読取部 3 1 を用いて指紋情報を読み取る機能を達成する C P U 等よりなる制御部 3 4 とを具備して構成されている。ホスト P C 3 0、4 0 はスキャナ X に対して、操作者が指定した読取条件に基づいて原稿画像を読み取らせ、更に読み取った原稿画像情報を操作者が操作するホスト P C に返信する旨の指令（以下、「操作指令」と称す）を送信する。

指紋読取部 3 1 は、ホスト P C 3 0 側で、少なくとも操作者の指紋情報を読み取るものであって、例えば特許文献 2 で示されているような指紋検出部付きマウス等がある。指紋情報記憶部 3 3 は、指紋読取部 3 1 で読み取られた指紋情報を一時的に記憶するものであって、例えば、不揮発性メモリ等がある。

【 0 0 1 6 】

スキャナ X は、設定解除操作や原稿読取可能の旨を表示する操作表示部 1 0 と、操作者の指紋を読み取るための指紋読取部 1 1（第 1 の指紋情報読取手段の一例）と、上記指紋読取部 1 1 で読み取られた指紋情報を一時的に格納する指紋情報記憶部 1 5（第 1 の指紋情報記憶手段の一例）と、原稿がセットされているかどうかを検知する原稿センサ 1 2 と、セットされた原稿を読み取る原稿画像読取

部 1 3（原稿画像読取手段の一例）と、原稿画像が読み取り可能となってから所定の時間をカウントするタイマ 1 4 と、通信インターフェース部 1 6 と、上記各部を制御し、指紋情報読取機能（第 1 の指紋情報読取手段が達成）、指紋情報記憶機能（第 1 の指紋情報記憶手段が達成）、指紋情報照合機能（指紋情報照合手段が達成）、操作許可機能（操作許可手段が達成）、の各機能を実行する制御部 1 とを具備して構成されている。

ここで、スキャナ X の制御部 1 が実行する各種の機能について説明する。

第 1 の指紋情報読取手段が達成する指紋情報読取機能とは、スキャナ X 側で、少なくとも操作者の指紋情報を読み取る機能であって、例えば、スキャナ X 操作パネル（図 4 参照）に設けられている指紋読取部 1 1 で指紋を読み取るための機能である。

第 1 の指紋情報記憶手段が達成する指紋情報記憶機能とは、上記指紋読取部 1 1 により読み取られた指紋情報を一時的に記憶する機能であって、例えば、不揮発性メモリの一部領域が使用される。指紋情報照合手段が達成する指紋情報照合機能とは、上記スキャナ X 側の指紋情報記憶部 1 5 により記憶された指紋情報と、上記ホスト P C 側の指紋情報記憶部 3 3 により記憶された指紋情報とを照合する機能であって、例えば、指紋情報が合致するか否かの照合を実施するための機能である。操作許可手段が達成する操作許可機能とは、上記照合結果に基づいて、上記ホスト P C 3 0、4 0 で入力された操作指令による上記スキャナ X の操作を許可するための機能であって、上記照合により、指紋情報が合致したと判断された場合にスキャナ X の操作を許可するための機能である。

【 0 0 1 7 】

スキャナ X の制御部 1 は、更に原稿画像読取機能（原稿画像読取手段が達成）、関連情報作成機能（間接情報作成手段が達成）、関連情報記憶機能（関連情報記憶手段が達成）を具備するものでもある。

原稿画像読取機能とは、少なくとも上記スキャナ X へ操作指令を出す前に原稿画像を読み取る機能であり、関連情報作成機能とは、上記原稿画像読取部 1 3 により読み取られた原稿画像情報と、上記指紋読取部 1 3 により読み取られた指紋情報とを関連付けた関連情報を作成する機能であり、関連情報記憶機能とは、上

記関連情報を記憶する機能である。かかる各機能は後述する S 4 0 ～ S 7 0 の画像処理を実現し、原稿画像情報の盗難防止を図るための機能である。

また、スキャナ X の制御部 1 は、更に関連情報消去機能（関連情報消去手段が達成）を具備するものである。

関連情報消去機能とは、上記のように指紋情報の照合がなされた場合に、操作終了指令後に上記関連情報を消去する機能であって、スキャナ X の操作終了後に、指紋情報記憶部に記憶されていた指紋情報等を消去することで、個人の重要な指紋情報の外部流出の危険性を排除する機能である。

【0018】

次に、図 2 を用いて、本発明の実施の形態に係る画像処理システムにより実行される原稿画像の読み取りを行う処理手順の一例を説明する。図 2 は上記手順を示すもので、大きく分けてスキャナ X 側において行われる処理（S 1 0，S 2 0，…で示される）とホスト P C 3 0 側において行われる処理（S 3 1，S 3 2，…で示される）とに分けられる。

なお、図中の S 1 0，S 2 0 …は処理手順（ステップ）番号を示す。処理はステップ S 1 0 より開始される。

【0019】

操作者によりスキャナ X で読み取る原稿が、スキャナ X の原稿画像読取部 1 3 にセットされると（S 1 0），制御部 1 は、原稿センサ 1 2 により原稿がセットされたことを検知して（S 2 0），次いで操作者の指紋情報の読み取りを開始する。指紋情報は例えば図 5（a）に示されるように、スキャナ X の操作パネルに設けられた指紋読取部 1 1 に、操作者の所定の指紋を接触させることで読み取られる（S 3 0）。ここで読み取られた指紋情報は指紋情報記憶部 1 5 に一時的に記憶される（S 3 0）。

【0020】

S 3 0 の処理が終了すると、操作者はホスト P C 3 0 に移動し、ホスト P C 3 0 からスキャナ X に対して操作指令を出す。

操作者はホスト P C 3 0 側で、スキャナドライバを選択し（S 3 1），その後、操作者はホスト P C 側で自己の指紋情報を読み取らせる（S 3 2）。ここで読

み取られた指紋情報は指紋情報記憶部 3 3 に一時的に記憶される（S 3 2）。指紋情報はホスト P C 3 0 側に設けられた指紋読取部 3 1 に、操作者の指紋を接触させることにより読み取られる。続いて操作者は原稿画像の読取を開始すべくスキナ X に対して操作指令を送信する（S 3 3）。S 3 3 における操作指令は、S 3 2 において指紋が読み取られると同時に行われることが望ましく、そうすることで、操作指令入力作業が省略され、操作性を高めることができる。

スキナ X が有する制御部 1 は、ホスト P C 3 0 から S 3 2 で読み取られた指紋情報及び S 3 3 の操作指令があったかどうかを S 5 0 で判断する。指紋情報及び操作指令の双方が入力されたと判断した場合は、S 3 0 で読み取られた指紋情報と、S 3 2 で読み取られた指紋情報とを照合する（S 6 0）。S 6 0 において双方の指紋が一致すると判断された場合は、スキナ X に原稿をセットした操作者自身がホスト P C 3 0 からスキナ X を操作していると判断できるので、原稿の存在を確認した後、操作者が要求した読み取り条件に基づいて原稿画像の読み取りを開始し、読み取りが完了すると、読み取り操作指令が出されたホスト P C 3 0 に対して、読み取られた原稿画像情報を送信する（S 7 0）。なお、原稿センサ 1 2 による原稿の検出は、後述 S 8 0 において、操作終了指令があると判断されるまで継続して行われることにより、操作者が所望する読取条件下における読み取りが行われる。

S 7 0 で送信された原稿画像情報は、ホスト P C 3 0 において受信され（S 3 4）、操作者はその画像を確認し、所望の画像を得た場合はスキナ X に操作終了指令を送信する（S 3 5）。操作終了指令を送信した場合は、ホスト P C の制御部 3 4 は、指紋情報記憶部 3 3 から操作者の指紋情報を削除し、スキナ X が該操作終了指令を受信した場合は（S 8 0）、スキナ X の制御部 1 は、指紋情報記憶部 1 5 から操作者の指紋情報を削除する（S 9 0）。その後画像処理が終了する。

スキナ X が具備するタイマ 1 4 は、S 3 0 において指紋情報が読み取られた後からカウントを開始し、S 8 0 で操作終了指令があると判断するまでの間カウントをし続け、所定の時間が経過した場合は、上述の S 9 0 の処理の後に、一連の画像処理を強制中断させる。

【0021】

【実施例】

上述の実施の形態では、スキャナX側及びホストPC30側で読み取られた指紋情報を、それぞれが持つ指紋情報記憶部15及び33に記憶させる場合について述べたが、本発明の画像処理システムは以下のような形態であっても良い。

例えば、スキャナX側及びホストPC30側で読み取られた指紋情報を、別途スキャナX及びホストPC30に通信接続可能なサーバ20（図1参照）の記憶部21に記憶するよう構成されていても良い。また、この場合、スキャナX側で読み取られた指紋情報と原稿画像読取部13で読み取られた原稿画像を関連付けてサーバ20の記憶部21に記憶することも考えられる。

以下に、図3及び図4を用いて、本実施例に係る画像処理システムにより実行される原稿画像の読み取りを行う処理手順を説明する。図3及び図4は上記手順を示すもので、上記実施の形態と同様に、大きく分けてスキャナX側において行われる処理（S110、S120、…で示される）とホストPC30側において行われる処理（S181、S182、…で示される）とに分けられる。

処理はステップS110より開始される。

操作者がスキャナXで読み取る原稿を、スキャナXの原稿画像読取部13にセットすると（S110）、制御部1は、原稿センサ12により原稿がセットされたことを検知して（S120）、次いで操作者の指紋情報の読み取りを開始する。指紋情報は例えば図5（a）に示されるように、スキャナXの操作パネルに設けられた指紋読取部11に、操作者の所定の指紋を接触させることで読み取られる（S130）。ここで読み取られた指紋情報は一旦サーバ20の記憶部21に一時的に記憶される（S130）。

S130で操作者の指紋情報が読み取られると、続いて、制御部は原稿画像読取部13にセットした原稿を一度読取走査する。ここでも読み取られた原稿画像は上記指紋情報と同様にサーバ20の記憶部21に記憶される（S140）。かかる原稿画像の読み取りは、S130で操作者の指紋情報が読み取られると同時に行うことが望ましく、そうすることにより指紋情報と原稿画像の読取作業を一の手順で行うことができる。

S130, S140で読み取られた指紋情報及び原稿画像は、制御部1が具備する関連情報作成機能により作成された過去の関連情報と照合される(S150)。S150で行われる照合は、まずS160において、読み取られた原稿画像が過去に作成された関連情報に含まれる画像情報と一致するかどうか判断される。ここで、原稿画像が過去の関連情報に含まれる画像情報と一致しない場合は、S170に進み、読み取られた操作者の指紋情報と原稿画像情報とを制御部1が具備する関連情報作成機能により関連付けて、サーバ20の記憶部21に記憶し、その後S180に進む。前記実施の形態では、スキャナXに関連情報が記憶されるので、盗難にあった原稿が別のスキャナXから読み取られることを防止できないが、このように関連情報がスキャナX側ではなくサーバ20側に記憶された場合には、複数のスキャナのどれが使用されても、その原稿画像をサーバ20側に蓄積された未処理画像と照合されるので、後述するように盗難にあった原稿がいずれかのスキャナで読み取られた時点で盗難原稿の判別が可能となる。

S160において、原稿画像が過去の関連情報に含まれる画像情報と一致し、操作者の指紋情報も過去の関連情報に含まれる指紋情報と一致すると判断された場合は(S161)、そのままS180に進む。既に、過去に同一の関連情報が作成され、サーバ20の記憶部21に削除されず記憶されているので、新たに関連情報を作成する必要がないからである。またこの場合、S161では、操作者の指紋情報と過去の関連情報に含まれる指紋情報とが一致しないと判断された場合は、別人による原稿画像の読み取りが行われようとしていると判断され、原稿が盗難原稿であると判別され、該原稿の読み取りが不可能である旨の表示(盗難原稿であることを報知するものでも良い)等をした後に(S162)、スキャナXの画像処理が終了する。

S180では、制御部1はスキャナXにセットされた原稿が読み取り可能である旨の表示等を行い(図5(b)参照)、かかる表示を確認すると操作者はホストPC30に移動し、ホストPC30からスキャナXに対して操作指令を出す。

【0022】

操作者はホストPC30側で、スキャナドライバを選択し(S181)、その後、操作者はホストPC側で自己の指紋情報を読み取らせる(S182)。指紋

情報はホストPC30側に設けられた指紋読取部31に、操作者の指紋を接触させることにより読み取られる。続いて操作者は原稿画像の読取を開始すべくスキャナXに対して操作指令を送信する(S183)。S183における操作指令は、S182において指紋が読み取られると同時に行為れることが望ましく、そうすることで、操作指令入力作業が省略され、操作性を高めることができる。

スキャナXが有する制御部1は、ホストPC30からS182で読み取られた指紋情報及び、S183の操作指令があったかどうかをS200、S210で判断する。指紋情報及び操作指令の双方が入力されたと判断した場合は、S120で読み取られた指紋情報と、S210で読み取られた指紋情報とを照合する(S120)。S230において双方の指紋が一致すると判断された場合は、再度原稿の有無をチェックし(S240)、その後、操作者が要求した読み取り条件に基づいて原稿画像の読み取りを開始し、読み取りが完了すると、読み取り操作指令が出されたホストPC30に対して、読み取られた原稿画像情報を送信する(S250)。なお、S240の原稿有無のチェック処理は、S180において読取可能の表示がされた後からS260で操作終了指令があると判断するまでの間、継続して行為れることが好ましい。

S240において、原稿がないと判断された場合は、S241でその旨の警告(盗難発生の警告でもよい)をホストPCに送信すると共に、スキャナXの操作パネルの表示部10に表示する(図5(d)参照)。かかる場合、サーバに記憶された関連情報を消去せずに画像処理が終了する。

S250で送信された原稿画像情報は、ホストPC30において受信され(S184)、操作者はその画像を確認し、所望の画像を得た場合はスキャナXに操作終了指令を送信する(S186)。スキャナXが該操作終了指令を受信した場合は(S260)、スキャナXはサーバ20の記憶部21から原稿画像に対応する関連情報を削除した後(S270)、画像処理が終了する。これにより、指紋情報が漏出する問題がなくなる。

スキャナXが具備するタイマ14は、S180において読取可能の表示がされた後からカウントを開始し、S260で操作終了指令があると判断するまでの間カウントをし続け、所定の時間が経過した場合は、制御部1が上述のS270の

処理の後にスキャナ X の画像処理を強制中断させる。更に、所定の時間が経過したときに、画像処理を強制中断させる旨の警告をホスト P C に送信すると共に、スキャナ X の操作パネルの表示部 10 に表示（図 5（c）参照）するようにすれば操作者にとって親切である。

【0023】

上述の実施例では、サーバ 20 内の記憶部 21 に指紋情報、原稿画像情報、関連情報を記憶する形態について説明したが、係る記憶部 21 はサーバが保有するものに限るわけではなく、ネットワーク接続環境下においてスキャナ X 及びホスト P C と通信接続可能な記憶装置が保有する形態であっても問題はない。

また、上記指紋情報、原稿画像情報及び関連情報を同一記憶部に格納する必要性もなく、例えば指紋情報と原稿画像情報とをスキャナ X やホスト P C 内のハードディスクやメモリ等の記憶部に一時的に格納し、それらが関連付けられた関連情報だけを、他のネットワーク上の記憶装置等に記憶するものであってもよい。なお、かかる場合、一時記憶されていた指紋情報及び原稿画像情報は関連情報が作成されることにより消去されることが望ましい。

また、原稿画像読取部 13 について述べたが、該原稿画像読部 13 は所定の解像度で原稿画像を読み取るものであっても良い。例えば低解像度で読込むことによって、読込み時間が短縮され、スムーズな画像処理を実現することができる。

更に、原稿画像を O C R 処理することで、原稿に含まれる文字情報のみを抽出して読み取るものも考えられる。スキャナで読み取られる対象には、写真や画像のみならずテキスト等も考えられるからである。この場合、かかるテキスト情報からキーワードを抽出して、該キーワードと関連情報とを照合することにより原稿画像を照合することも効果的である。

更にまた、原稿を複数のブロックに分割して読み取ることも考えられる。原稿をセットする向きや範囲等によっては、単に読取走査するだけでは同一原稿であっても別個のものと判断される可能性が高いため、原稿を複数のブロックに分割して読み取り、例えば分割された一部が、関連情報に含まれる画像情報の一部と一致する場合に同一原稿として判断することにより、原稿画像を照合することも効果的である。

【 0 0 2 4 】

【発明の効果】

以上説明したように、本発明によれば、例えばスキャナ側で読み取られた指紋情報と、操作者が使用している端末装置側で読み取られた指紋情報とを照合することで、予め指紋情報を保存登録する必要のない且つ、スキャナの操作者を限定することのない画像処理システムを構築することが可能となるばかりでなく、他の操作者が原稿画像を読み込む行為を有効に禁止することができる。

更には、スキャナ操作終了後に記憶された指紋情報等を消去することで、個人の重要な指紋情報が長期保存されることがなくなるため、指紋情報の外部流出の危険性を極力低減させ、指紋情報を長期保存することから生じる指紋情報の持ち主の不安も解消させる効果を奏し、高いセキュリティ性と操作性を獲得することができる。

【図面の簡単な説明】

【図 1】 本発明の実施の形態に係る画像処理システムの全体構成を表すブロック図。

【図 2】 本発明の実施の形態に係る画像処理システムにより実行される原稿画像の読み取りを行う処理手順を表すフローチャート。

【図 3】 本発明の実施例に係る画像処理システムにより実行される原稿画像の読み取りを行う処理手順を表すフローチャート。

【図 4】 本発明の実施例に係る画像処理システムにより実行される原稿画像の読み取りを行う処理手順を表すフローチャート。

【図 5】 本発明の実施の形態に係る画像処理システムに用いられるスキャナ X の操作パネルの一例を表した図。

【符号の説明】

- 1…制御部
- 10…操作・表示部
- 11…指紋読取部
- 12…原稿センサ
- 13…原稿画像読取部

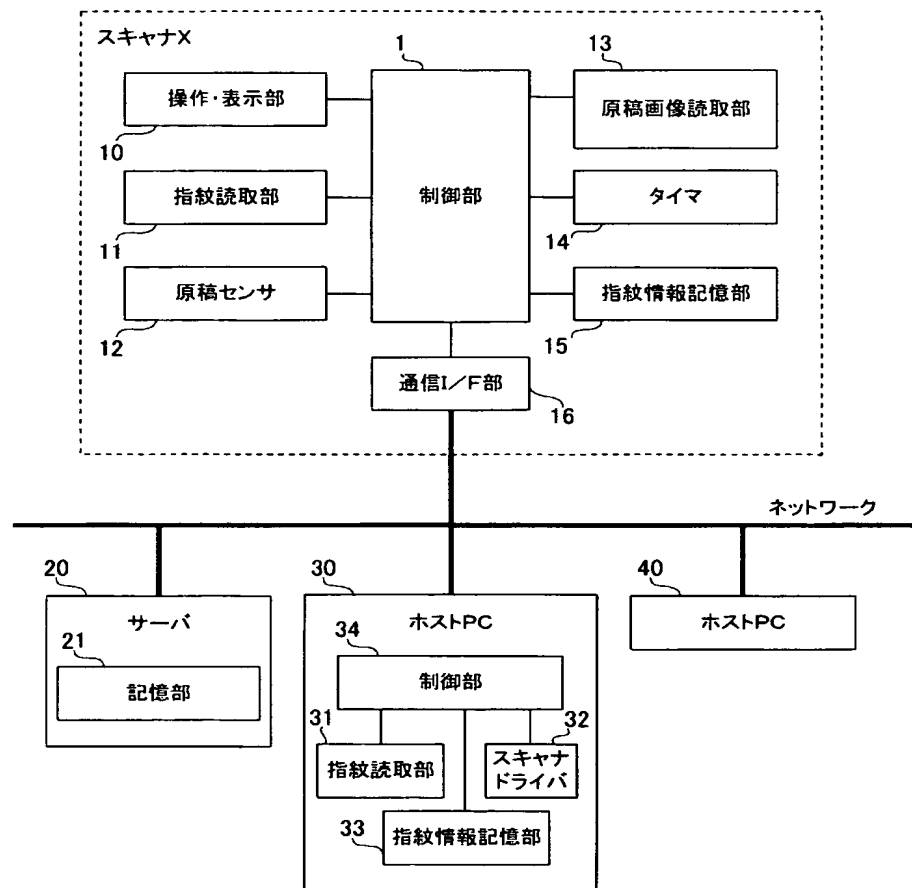


- 1 4 … タイマ
- 1 5 … 指紋情報記憶部
- 1 6 … 通信インターフェース
- 2 0 … サーバ
- 2 1 … 記憶部
- 3 0, 4 0 … ホスト P C (端末装置の一例)
- 3 1 … 指紋読取部
- 3 2 … スキャナドライバ
- 3 3 … 指紋情報記憶部
- 3 4 … 制御部

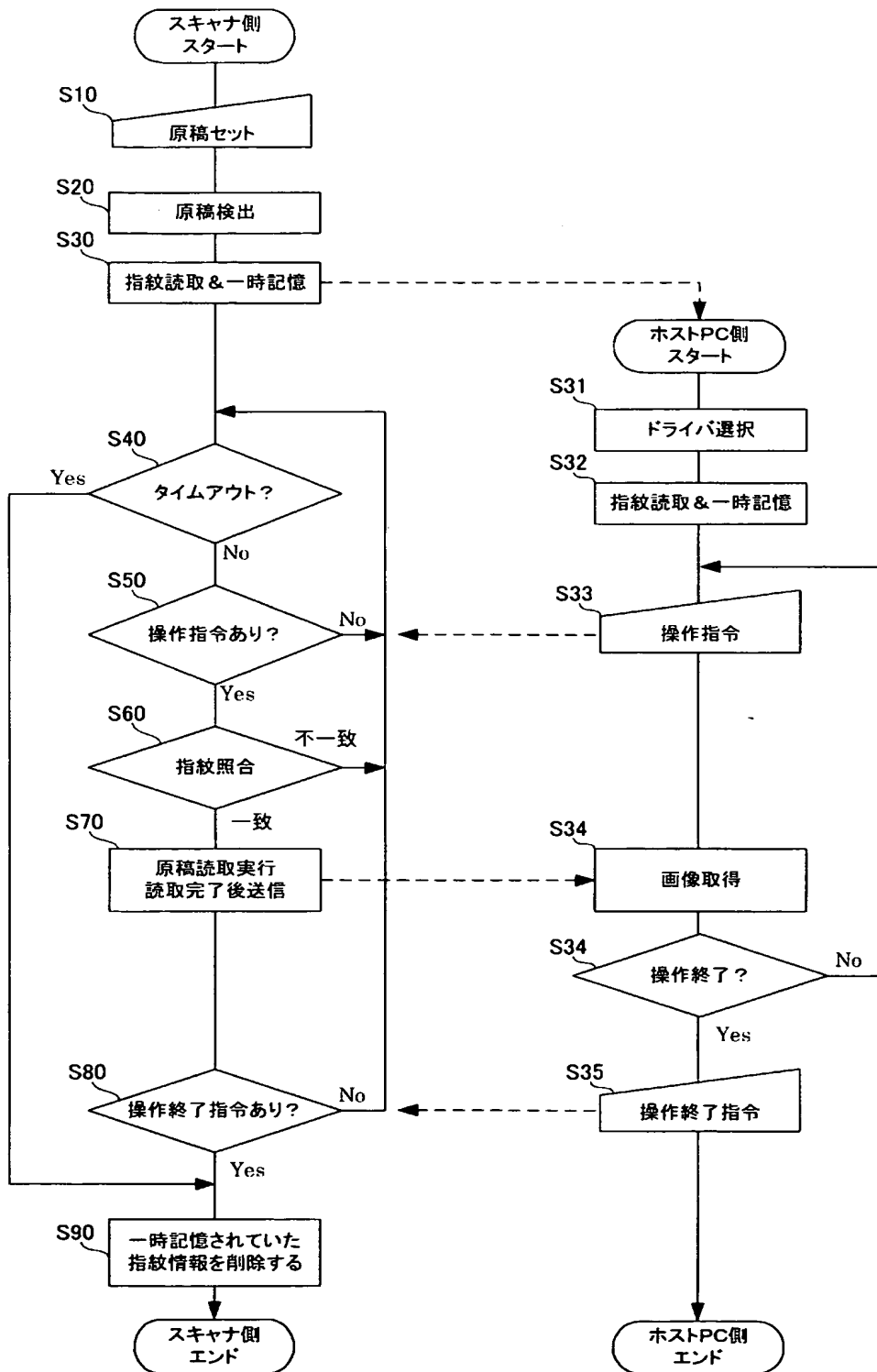
【書類名】

図面

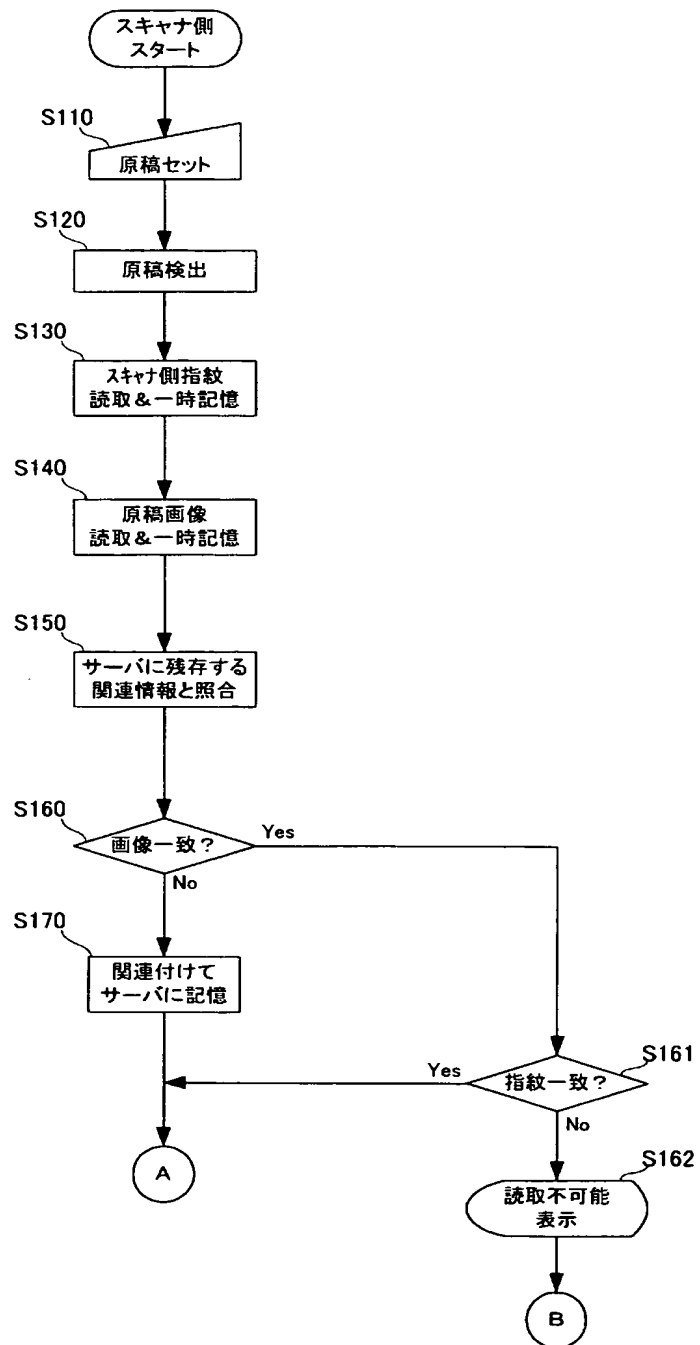
【図 1】



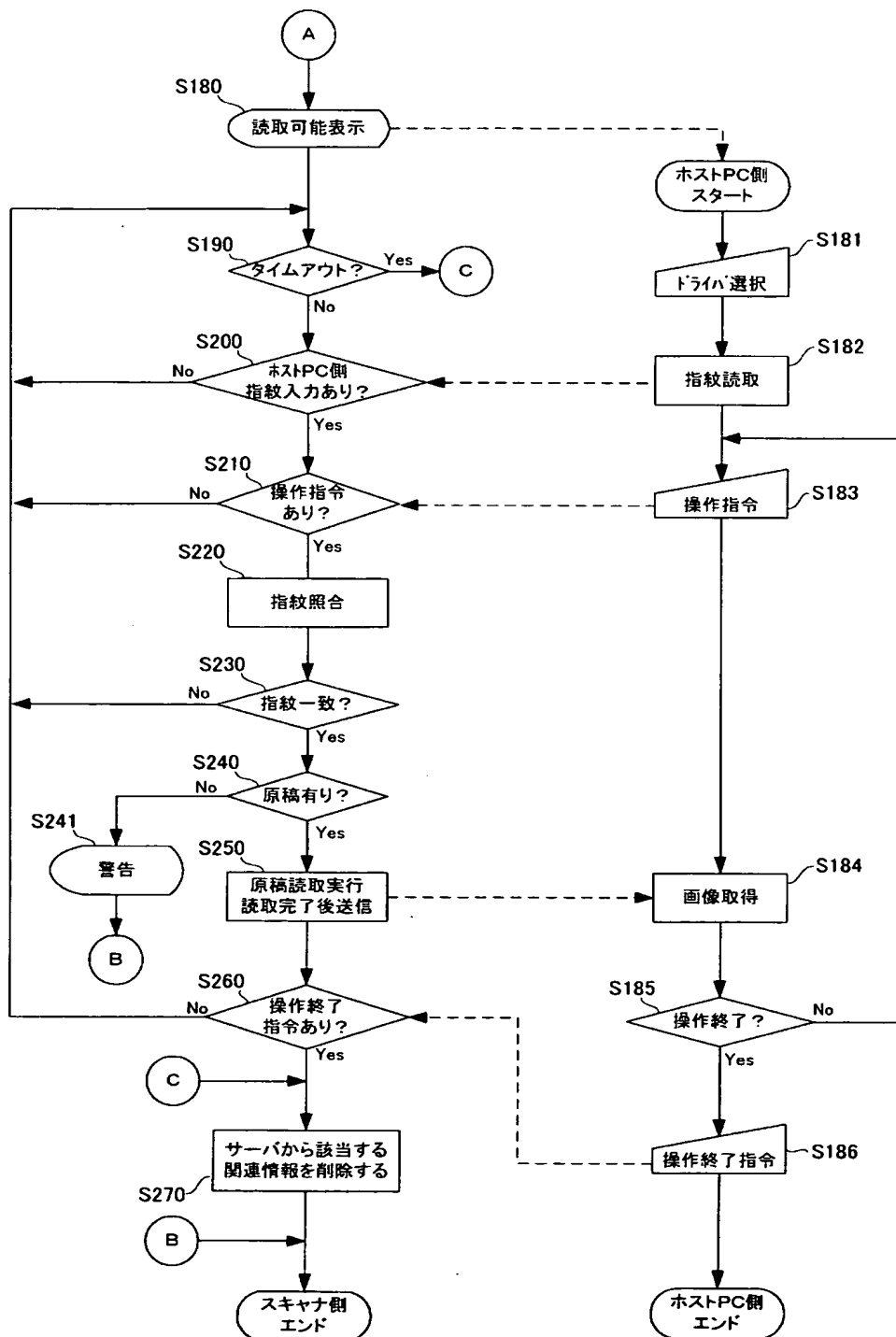
【図 2】



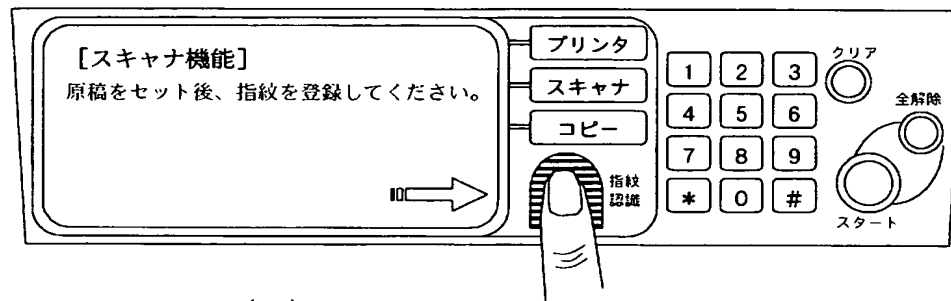
【図 3】



【図 4】



【図 5】



(a)

[スキャナ機能]
指紋が登録され、スキャナの予約を行ないました。
ホストからスキャン指示することで、
画像を読み取ることが出来ます。

(b)

[スキャナ機能]
タイムアウトによりスキャナの予約を取り消しました。
原稿を取り除いてください。

(c)

[スキャナ機能]
原稿が取り除かれました。
原稿を確認してください。

(d)

【書類名】 要約書**【要約】**

【課題】 従来の指紋情報を利用した画像処理装置は、操作者の指紋情報を予め保存登録しておく必要があった。しかし、保存された指紋情報が外部に流出する危険性が伴い、更には指紋情報登録者だけしか該画像処理装置を使用できないという問題があった。

【解決手段】 本発明は、例えばスキャナ側で読み取られた指紋情報と、操作者が使用している端末装置で読み取られた指紋情報とを照合し、その照合結果に基づいて操作者に対して上記スキャナ装置の使用を許可することにより、操作者を限定せず、何人も上記スキャナを使用することができることとした。

更には、上記照合するために一時的に記憶させた指紋情報等を、上記スキャナ装置の使用終了後に消去し、重要な個人情報である指紋情報を長期保存しないことにより、指紋情報の外部流出の危険性を排除した。

【選択図】 図 1

特願 2 0 0 2 - 3 2 1 5 8 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 0 4 9]

1 . 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

大阪府大阪市阿倍野区長池町 2 2 番 2 2 号

氏 名

シャープ株式会社